HIT Policy Committee
NHIN Workgroup

Remarks of Judith Spencer

1. What trust problems are you trying to solve and for what range of users (e.g. organizations, individuals, health care professionals, consumers)? Please provide some quantitative data if possible to characterize your user base (e.g., percentage or number of each type).

It has been understood since the mid-1990s that reliable on-line identity assurance was a key enabler of electronic government. Without the appropriate level of trust in the asserted identity and the 'credentials' presented to assert that identity, meaningful business transactions cannot take place. This was recognized again in the Cybersecurity Review completed in early 2009. The drivers for effective identity management activities include protecting the privacy of individuals, protection of Federal systems and information, and prevention of cybercrime. The Identity, Credential, and Access Management (ICAM) subcommittee of the Federal Chief Information Officers (CIO) Council Information Security and Identity Management Committee (ISIMC) is the government-wide body coordinating the Federal activities in the area of establishing a set of solutions that can be leveraged across agency boundaries for doing business internally, between the Federal government and other governments (state, local, tribal, allied), with the commercial sector, and with the American people. Each of these communities presents different challenges and demands; the most challenging being the interaction with the American people, a population of approximately 230 million individuals over the age of 18[1], any one of whom may wish to access Federal services electronically at any time. The ICAM concerns itself with the Federal government as a Relying Party and, to a lesser extent, the Federal government as an identity provider. We take our energy from the activities of the past, beginning with the Government Paperwork Elimination Act of 1998 and the E-Government Act of 2002, further defined by Office of Management and Budget (OMB) Policy Memorandum M-04-04 "E-Authentication Guidance for Federal Agencies" which introduces four levels of assurance for identity beginning with the baseline Identity Assurance Level 1: "No confidence in the real world identity"; and ending with Identity Assurance Level 4: "Very high confidence in the real world identity." These four levels of identity assurance are linked to Federal Information Processing Standard (FIPS) 199 Risks and Impacts for damage that can be suffered due to providing information or services based on a 'false positive' access control decision or, conversely, denial of access to information or services based on a 'false negative' access control decision. These risks and impacts range from inconvenience to personal safety and map to the four levels of identity assurance, which in turn map to the type and strength of the credential that must be used to assert identity and the procedures used to establish the validity of the claimed identity and the claimant's right to the identity in order to bind that identity to the claimant's credential. OMB M-04-04 requires Federal agencies to determine the identity risks and impacts of their electronic services and assign the appropriate level of identity assurance. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 provides guidance on the minimum identity management solutions that must be implemented for each level of identity assurance. Any business process for which the risk in any one of the six risk and impact areas of identity management is high

[1] Source: US Census Bureau statistics "Resident Population by Sex and Age" current as of July 1, 2008. http://www.census.gov/compendia/statab/2010/tables/10s0007.pdf

is a Level 4 system for identity assurance and must be protected accordingly. SP 800-63 requires a hardware token-based cryptographic identity credential for access control at Level 4.

For the Federal executive branch of government, strong identity credentialing for the workforce that can be leveraged for access control and enabling business processes has been achieved through Homeland Security Presidential Directive (HSPD) 12 and the subsequent FIPS 201: "Personal Identity Verification of Federal Employees and Contractors". This Personal Identity Verification (PIV) credential has been issued to over 75% of the Federal workforce and its contractors (4.3 million people) and will soon be the primary means of access to facilities and logical systems both internal to departments and agencies and across agency boundaries. It provides Level 4 identity credentials strongly bound to individual identity with a means to establish validity of the credential real-time. Similar activities for strong credentials that are compatible with the PIV credential and technically interoperable with Federal systems are being undertaken by the states and industry.

However, this is only part of the story, while the benchmark for strong (Level 4) identity credentialing has been defined by HSPD-12 and FIPS 201, there is still a requirement to enable on-line business processes with less stringent identity requirements (Levels 1 through 3). To this end, we are pursuing solutions that take advantage of the industry standards in place for identity and access control in the commercial world. These range from the OpenID standard that has application at Level 1 identity assurance to One Time Password protocols that have potential to meet Level 3 identity assurance requirements. The goal is to leverage technology and activities already in place and to reuse credentials in use by businesses and individuals where appropriate. The ICAM Segment Architecture released in November 2009 as Part A of the ICAM Roadmap and Implementation Guidance further defines these activities and the ICAM goals of the Federal government. ICAM provides the policy and guidance for business process owners to ensure that the identification, authorization, and verification requirements are sufficient to enable the appropriate access to information, the delivery of service, protection of privacy, and integrity of the data.

2. Who pays for the solution, implementation, processes and support for your approach? What factors contribute to the total cost of ownership of the technologies, including process costs? What are the implications to widespread deployment?

To the extent possible, the ICAM Subcommittee is looking for ways to minimize costs for the implementation of strong identity solutions. Although not well defined, there are indications that the insertion and proper implementations of strong identity solutions have absolute effect on the total cost of ownership for both the individual and our business processes. The difficulty is that the return on investment (ROI) is spread over multiple applications and therefore challenging to define. Examples are the ability of the Department of Defense (DoD) to reduce network intrusions by 45% by the use of strong authentication or the ability of the U.S. Department of Agriculture (USDA) to integrate employee provisioning over their HR, IT security, and physical security plants. The 'capability of strong identity coupled with the network' became an enabler to combat fraud, network intrusions, and to launch changes in entrenched business processes. In each example, the enabled strong identity became the technical foundation for increased capability or cost reduction but built on the costly identity verification and credential system already in place.

Identity solutions are expensive but tend to be defined in a very narrow set of objectives. The ICAM is trying to illustrate that within a set community, a strong identity credential is a valued resource with ROI (network access and multiple applications, physical security,

travel, etc) and to promote the trust framework that allows us to make that investment portable across multiple business lines or communities. By reusing current credentials and technology solutions, requiring compatibility and technical interoperability, and providing clear guidance to the identity management technology sector, it is hoped that we can "solve once, use many times." Federal agencies are required by existing OMB policy to factor security costs into the life cycle of their investments. To this end, the agencies will be required to fund for the enabling of their processes and for upgrading systems where appropriate, but this one-time activity will pay dividends in the reduction of overhead to establish and maintain individual access control systems and manage password databases. We are currently looking into the capability of identity management systems to seamlessly process identity assertions from different sources using different identity solutions and protocols for making access control decisions, with excellent results.

When policies, law, technical capabilities, and business processes are inserted into a risk analysis, the outcome for credentialing requirements are normally quite clear. When those are weighted with the growing issues of fraud, data breach, and personal privacy there are very few secure and interoperable solutions available. The challenge is the use of very clear (and mature) technologies and the use of these technologies as the basis to form an identity infrastructure. For example, the definition of FIPS-201 from the existing processes and foundation of Public Key infrastructure (PKI) enabled a federated identity schema across the federal government by 21 providers instead of a single central identity card for the federal workforce. The balanced business deployment and having those closest to the 'customer' (i.e. federal employer) do identity proofing has proven a successful model. The case by the ICAM is that the technology, policy, and risk basis is documented and proven by the use of standards and standard processes and to federate those standards and processes is a proven and powerful approach.

3. Directory services often support some certificate authority or other authentication mechanism. As you look more broadly at the architecture, how do your approaches work with such directory services?

The use of directory services is an important and integral aspect of the solutions being developed via the ICAM activities. The ICAM Architecture Working Group has published technical specifications for back-end attribute exchange, which allows a relying party to request additional information concerning the role and privileges of an individual PIV credential holder in order to make an access control decision. Other directory services support the use of public key technology and verification of the validity of identity credentials at the time they are presented, providing real-time knowledge concerning the status of the identity credential, which in turn informs the access control decision-making process.

4. Does your approach support a delegated authentication model where there is an authorized registrar that issues the authentication credentials to individuals? If so, how? Are there implications for interoperability in this scenario?

Yes. This is a recognized business process necessity. The use of "trusted agents" to perform the identity verification and binding activity is an essential part of a large scale identity credentialing solution. In addition, the Federal Public Key Infrastructure (PKI) Policy Authority recently published a document on the use of an "In-person Antecedent" in further recognition of the realities of conducting business. In all cases, the convenience of the solution must be weighed against the need to maintain the appropriate control over the identity binding process to ensure the system cannot be subverted.

It is also important to note that an appropriately strong unique identity credential could be acquired by an individual for use in asserting identity which is then presented during a subsequent 'enrollment' process with a relying party and then bound to that individual's identity for future interactions with the relying party. For example: An individual visits a Federal website for the first time and wants to gain access to a controlled business application. He has in his possession a strong credential which he wishes to use for doing business with that Federal application. At the time of the initial visit, the Federal agency controlling the website needs to establish the identity of the individual in relation to its own records and data (e.g. the Internal Revenue Service may need to establish the connection between this individual and a specific tax record) in order to ensure it provides necessary services and/or to determine whether access to this business application is appropriate. To do so, the agency engages in a series of challenges to establish this relationship. Once the agency is satisfied that the linkage has been established and access is appropriate, it binds the strong credential presented by the individual to that record. On future visits, the presentation of the credential is recognized as bound to this identity. Other applications may result in establishing a linkage not based on previous data (e.g. an applicant applying for a grant). Appropriate enrollment processes will be used to establish a record for the individual, which is then bound to the presented credential. This is one possible scenario for the reuse of identity credentials, but is by no means the only option.

5. What should be the role of government? Where can rapid action address common concerns or limitations of trust?

Government can and must provide strong leadership in the establishment of standards and specifications for identity management, not only for the work with which the ICAM is concerned – the Federal government as a relying party or identity provider – but on a national scale among industry and between industry and the American public. The standards and specifications must emphasize trust and interoperability as key enablers in effective identity management. We have already seen several examples of this leadership in the activities undertaken by the Aerospace Defense Industry and the Bio-Pharmaceutical Industry, who independently determined that they would follow the Federal government's lead in establishing PKI solutions that not only emulate the Federal PKI Architecture but have also established trust relationships with the Federal government such that strong identity credentials issued by these two industry sectors can be trusted by Federal relying parties in conducting business, achieving both inter-organizational trust and interoperability of identity credentials.

We are laying the groundwork for extending this model beyond the confines for public key technology to the larger identity solution industry. A Trust Framework Evaluation process has been published along with an Identity Scheme Adoption process, both intended to assist in establishing standards and specifications. Participation in the activities of the ICAM and engaging in the debate concerning the trust fabric are important activities. Whether any of this lends itself to "rapid action" is undetermined. There is a need for a paradigm shift in how we approach the question of trust that can only be accomplished through a cultural change among the policy makers and organizational implementers, beginning with the realization that we do not have to do it all ourselves – it is possible to place trust in a presented identity claim, provided the appropriate validation processes have been implemented – trust but verify.